REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
07-05-2014

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
20 Mar 2013 – 19 Mar 2014

4. TITLE AND SUBTITLE

(134069) Ontology Assisted Assessment of Worldwide Cyber Research Trends

5a. CONTRACT NUMBER
FA23861314069

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Associate Prof. Kevin Barton

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Texas A&M University
One University Way
San Antonio, TX 78224
United States

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AOARD
UNIT 45002
APO AP 96338-5002

10. SPONSOR/MONITOR'S ACRONYM(S)

AOARD

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AOARD-134069

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research examined and reported on emerging global research trends in cyber security. The research defined a comprehensive set of cyber-related research concepts, which served as the basis for a cyber ontology relevant to current cyber concepts of interest to the Asian Office of Aerospace Research and Development (AOARD) office. This study was intended to strike a balance between automated searches of promising concepts using an operationally viable inferencing engine and manual reviews using the expertise of the research team. The overall objective was to use the strengths of each approach to gain insights gathered from refinement of the large data set associated with groundbreaking research underway globally. Results are presented in conjunction with a prototype web application. This prototype application provided visualization of the results, while also establishing an initial application framework intended for future expansion of the automated ontology assisted data gathering capabilities of this study.

15. SUBJECT TERMS

Computer Science, Computer Security Technology

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Brian Sells, Lt Col, USAF
U	U	U	UU	12	**19b. TELEPHONE NUMBER** *(Include area code)* +81-3-5410-4409

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **09 MAY 2014**	2. REPORT TYPE **Final**	3. DATES COVERED **20-03-2013 to 19-03-2014**

4. TITLE AND SUBTITLE **(134069) Ontology Assisted Assessment of Worldwide Cyber**	5a. CONTRACT NUMBER **FA23861314069**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Kevin Barton**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Texas A&M University,One University Way,San Antonio,TX,78224**	8. PERFORMING ORGANIZATION REPORT NUMBER **N/A**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) **AOARD, UNIT 45002, APO, AP, 96338-5002**	10. SPONSOR/MONITOR’S ACRONYM(S) **AOARD**
	11. SPONSOR/MONITOR’S REPORT NUMBER(S) **AOARD-134069**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research examined and reported on emerging global research trends in cyber security. The research defined a comprehensive set of cyber-related research concepts, which served as the basis for a cyber ontology relevant to current cyber concepts of interest to the Asian Office of Aerospace Research and Development (AOARD) office. This study was intended to strike a balance between automated searches of promising concepts using an operationally viable inferencing engine and manual reviews using the expertise of the research team. The overall objective was to use the strengths of each approach to gain insights gathered from refinement of the large data set associated with groundbreaking research underway globally. Results are presented in conjunction with a prototype web application. This prototype application provided visualization of the results, while also establishing an initial application framework intended for future expansion of the automated ontology assisted data gathering capabilities of this study.

15. SUBJECT TERMS

Computer Science, Computer Security Technology

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**3**	**12**	

Ontology Assisted Assessment of Worldwide Cyber Research Trends

April 16, 2014

Project Director/PI: Kevin Barton
Our Lady of the Lake University
411 SW 24th St
San Antonio, TX 78207

Co-PI: Matt Trippy
Enova Concepts LLC
11703 Huebner Road
Suite 106-230
San Antonio, TX 78230

Abstract: This research examined and reported on emerging global research trends in cyber security. The research defined a comprehensive set of cyber-related research concepts, which served as the basis for a cyber ontology relevant to current cyber concepts of interest to the Asian Office of Aerospace Research and Development (AOARD) management team. This study was intended to strike a balance between automated searches of promising concepts using an operationally viable inferencing engine and manual reviews using the expertise of the research team. The overall objective was to use the strengths of each approach to gain insights gathered from refinement of the large data set associated with groundbreaking research underway globally. Results are presented in conjunction with a prototype web application. This prototype application provided visualization of the results, while also establishing an initial application framework intended for future expansion of the automated ontology assisted data gathering capabilities of this study.

Ontology Assisted Assessment of Worldwide Cyber Research Trends
BAA-AFOSR-2012-0001

Background

The research described in this report is intended to enhance Asian Office of Aerospace Research and Development (AOARD) objectives to provide outreach and support to researchers across Asia and the Pacific Rim by examining and reporting emerging global research trends in cyber security.

Our intent was to bring two primary capabilities to bear on the large and diverse set of cyber research taking place globally, with the result of shaping a deeper inspection into promising pockets of research. The results should provide AOARD the potential of effecting significant impacts on future security of networks, networked systems, and the information being protected. The first capability explicitly defined a comprehensive set of cyber-related research concepts which were then used as the basis for a cyber ontology relevant to current cyber concepts of interest to the AOARD management team. The second capability was the employment of the deep expertise of the cyber team at the Computer Information Systems and Security (CISS) department at Our Lady of the Lake University (OLLU), which develops and delivers instructional programs. OLLU is an NSA/DHS designated Center of Academic Excellence in Information Assurance Education (CAE-IAE). OLLU's research into critical areas of cyber defense capabilities afforded the team unique expertise that greatly enhanced the products and processes of this research project.

This study was purposed to strike a balance between automated searches of promising concepts using an operationally viable inferencing engine, and direct use of the high expertise of the OLLU research team. Automated searches have been applied to information security research in recent years, including a web crawling methodology (Watters, Layton, & Dazeley, 2011) and development of fuzzy decision support systems (Schryen, 2010). The expertise of the team was focused on gaining insights gathered from the process of refinement of the large data set associated with groundbreaking research underway globally.

Approach

Our starting point for a concept map was derived from multiple sources, including Air Force stated needs identified in "Cyber Vision 2025" (AF/ST TR 12-01 dated 15 Jul 2012), the "Report on Technology Horizons, A Vision for Air Force Science & Technology During 2010-2030", internal research team brainstorming sessions, and feedback from AOARD and other key research managers with a direct interest in the proposed research. The final summary level concept map for Worldwide Cyber Research Trends is shown in Figure 1.

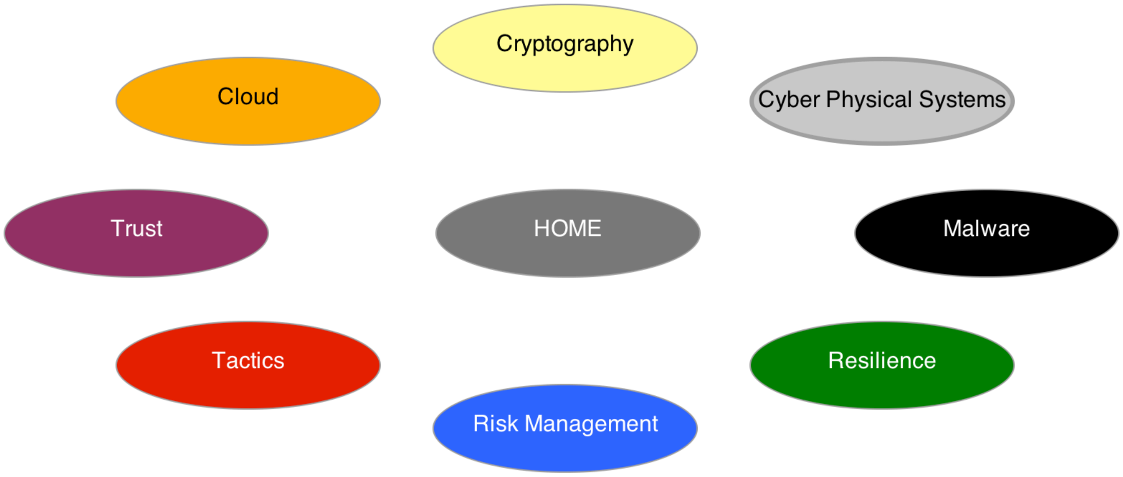


Figure 1. Final (Summary) Concept Map for Worldwide Cyber Research Trends

In order to enable more interactive review by AOARD researchers, this summary level visualization of the cyber ontology was crafted into a browser-based application. The summary level screen is the entry point to multiple screens of data displaying the more detailed ontology that resides within each top-level concept shown in Figure 1.

Further, we captured the key concept metrics in both concept-oriented visualizations, as illustrated in Figure 2, and geomap visualizations, as shown in Figure 3. A full, interactive visualization of the full data set is available with the application prototype delivered to AOARD personnel and available at http://cims.enovations.org . The detailed concept maps were in place to show the relative abundance of research in each of the 8 areas of interest, drilled-down into multiple sub-level concepts. The AOARD user requirements were seen as twofold. Researchers would have a need to understand the full extent of these concepts, through the display of technical paper titles, as well as a further drill-down to individual abstracts. The AOARD team would also expect a geomap visualization of these papers, in order to more quickly identify subject areas and individual technical papers that would indicate relative strength of individual universities and researchers. This second requirement led to the development of the map based views using open source mapping API's, and individual maps provided by interfacing with both Google Maps and OpenStreets mapping servers.

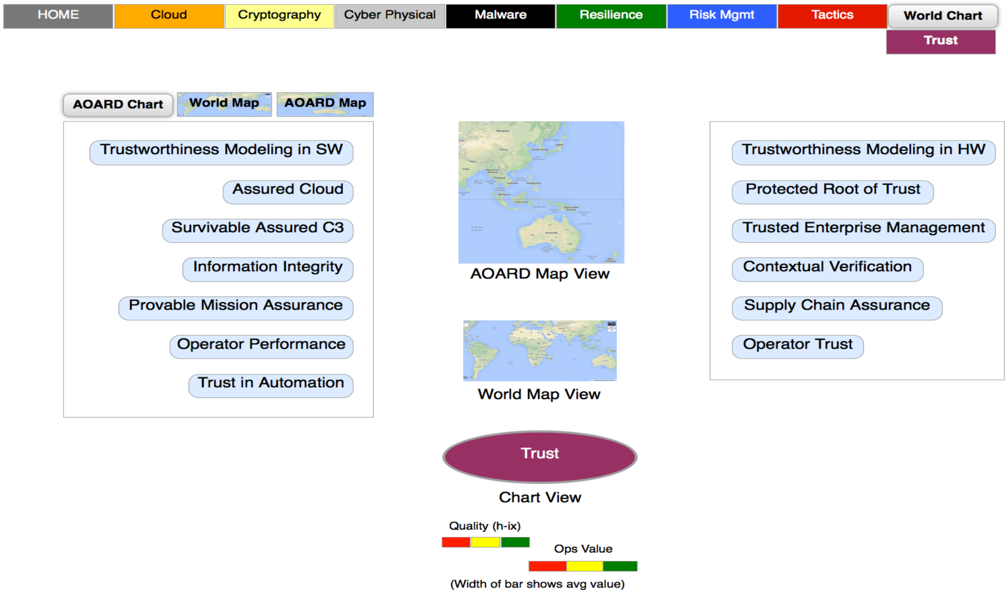


Figure 2: Detailed Concept Map Visualization of Worldwide Cyber Research Trends

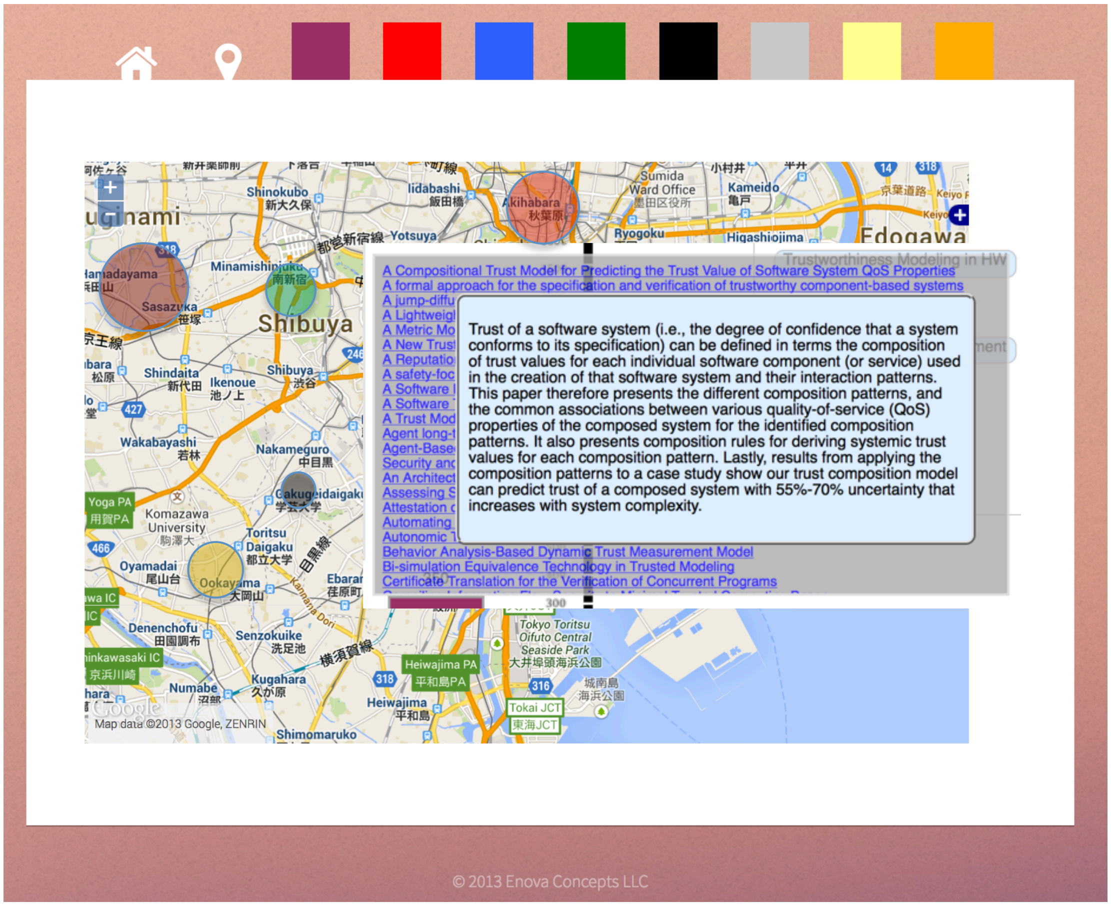
Note that the circles shown on the (notional) map in Figure 3 are intended to display, by relative size, a combination of researcher quality index, and the operational relevance of the paper, as determined by "ops scoring". Researcher h-index is normalized to a 1 to 5 scale. This metric constitute 50% of the circle's radius. The remaining 50% is a one to 5 scaled "Ops score", determined by the factors shown in Table 1 below:

Table 1. Operations Evaluation Criteria

Criteria	Descriptions	1	2	3	4	5
Assure & Empower the Mission	Mission awareness from managed information. Assured mission operations in a cloud environment with self-protecting information. Empower access control and D5 effects.	Restates already understood factors of mission awareness, cloud operations or D5, but does not add new clarity or knowledge.	Adds new clarity to generally well understood factors related to mission awareness, cloud operations or D5, but does not advance knowledge in a new direction or capability.	Supports, supplements, or advances an emerging research stream related to mission awareness, cloud operations or D5.	Closes significant gaps in an emerging research stream related to mission awareness, cloud operations or D5.	Initiates or significantly advances new and exciting knowledge related to mission awareness, cloud operations or D5.
Optimize Human Machine Systems	Measure and achieve operator trust in automation, operator vigilance and	Restates already understood factors of operator trust in automation, operator	Adds new clarity to generally well understood factors related to operator trust in	Supports, supplements, or advances an emerging research stream related to operator	Closes significant gaps in an emerging research stream related to operator	Initiates or significantly advances new and exciting knowledge related to operator trust in automation, operator vigilance and stress, operator performance

	stress. Predict operator performance. Understand and predict adversary reasoning.	vigilance and stress, operator performance prediction, and understanding adversary reasoning.	automation, operator vigilance and stress, operator performance prediction, and understanding adversary reasoning.	trust in automation, operator vigilance and stress, operator performance prediction, and understanding adversary reasoning.	trust in automation, operator vigilance and stress, operator performance prediction, and understanding adversary reasoning.	prediction, and understanding adversary reasoning.
Enhance Agility and Resilience	Resilience through anticipatory defense, tamper resistance and self-healing networks. Agile VM replacement Agility through cloud virtualization	Restates already understood factors of resilience, anticipatory defense, self-healing networks, agile VM replacement and cloud virtualization.	Adds new clarity to generally well understood factors related to resilience, anticipatory defense, self-healing networks, agile VM replacement and cloud virtualization.	Supports, supplements, or advances an emerging research stream related to resilience, anticipatory defense, self-healing networks, agile VM replacement and cloud virtualization.	Closes significant gaps in an emerging research stream related to resilience, anticipatory defense, self-healing networks, agile VM replacement and cloud virtualization.	Initiates or significantly advances new and exciting knowledge related to resilience, anticipatory defense, self-healing networks, agile VM replacement and cloud virtualization.
Foundations of Trust	Reverse engineering and vulnerability analysis tools. Supply chain assurance; threat avoidance. Quantitative risk modeling Provable mission assurance in contested cyber domain	Restates already understood factors of reverse engineering, vulnerability analysis, supply chain assurance, threat avoidance, risk modeling and provable mission assurance.	Adds new clarity to generally well understood factors related to reverse engineering, vulnerability analysis, supply chain assurance, threat avoidance, risk modeling and provable mission assurance.	Supports, supplements, or advances an emerging research stream related to reverse engineering, vulnerability analysis, supply chain assurance, threat avoidance, risk modeling and provable mission assurance.	Closes significant gaps in an emerging research stream related to reverse engineering, vulnerability analysis, supply chain assurance, threat avoidance, risk modeling and provable mission assurance.	Initiates or significantly advances new and exciting knowledge related to reverse engineering, vulnerability analysis, supply chain assurance, threat avoidance, risk modeling and provable mission assurance.

This “Ops score” was preserved in the tagging field of the AOARD group that was created within Mendeley, a researcher tool for storing and sharing technical research of interest. Mendeley was also used as the repository of query results, and was accessed programmatically (through a developer API) in order to populate the web-based prototype with the final results.



A Compositional Trust Model for Predicting the Trust Value of Software System QoS Properties
A formal approach for the specification and verification of trustworthy component-based systems
A jump-diffu
A Lightweigl
A Metric Mo
A New Trust
A Reputatio
A safety-foc
A Software I
A Software
A Trust Mod
Agent long-t
Agent-Base
Security and
An Architect
Assessing S
Attestation c
Automating
Autonomic T
Behavior Analysis-Based Dynamic Trust Measurement Model
Bi-simulation Equivalence Technology in Trusted Modeling
Certificate Translation for the Verification of Concurrent Programs

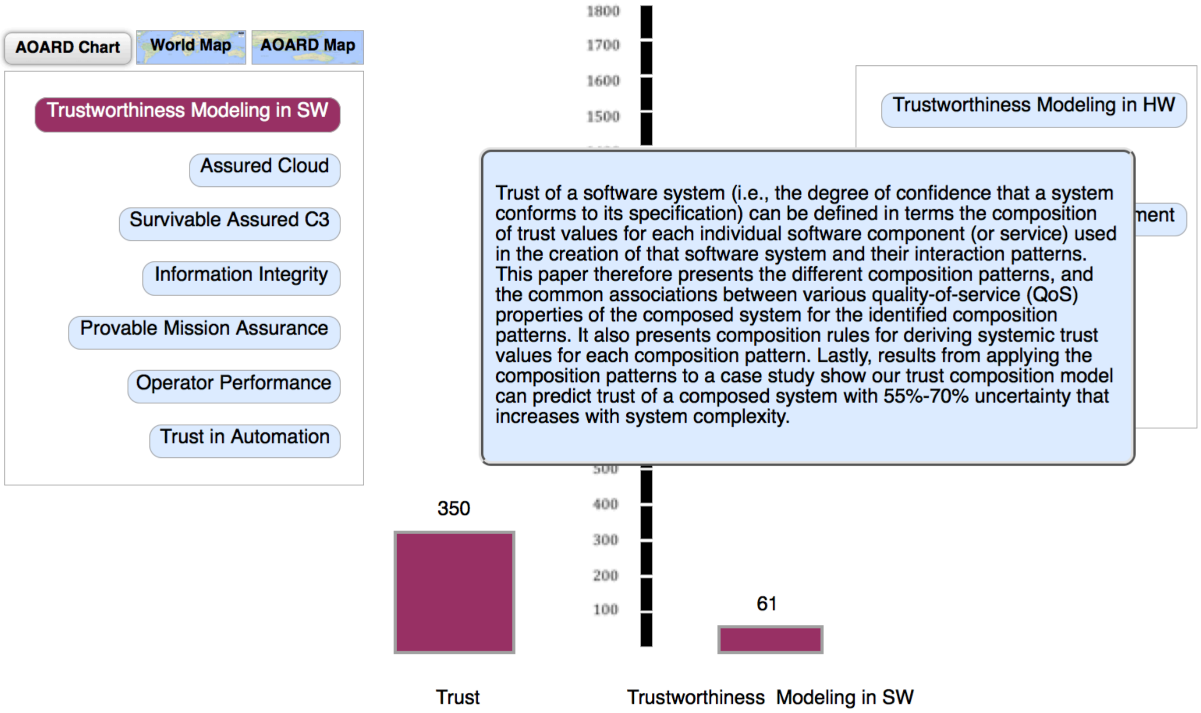
Trust of a software system (i.e., the degree of confidence that a system conforms to its specification) can be defined in terms the composition of trust values for each individual software component (or service) used in the creation of that software system and their interaction patterns. This paper therefore presents the different composition patterns, and the common associations between various quality-of-service (QoS) properties of the composed system for the identified composition patterns. It also presents composition rules for deriving systemic trust values for each composition pattern. Lastly, results from applying the composition patterns to a case study show our trust composition model can predict trust of a composed system with 55%-70% uncertainty that increases with system complexity.

© 2013 Enova Concepts LLC

Figure 3. Interactive Geomap Visualization of Worldwide Cyber Research Trends (zoomed in view)

Results

The bar graphs for each of the 8 concept areas are displayed in the associated prototype application. Figure 4 shows one of the subcategories of the "TRUST" concept area extracted from this prototype application.



Trust of a software system (i.e., the degree of confidence that a system conforms to its specification) can be defined in terms the composition of trust values for each individual software component (or service) used in the creation of that software system and their interaction patterns. This paper therefore presents the different composition patterns, and the common associations between various quality-of-service (QoS) properties of the composed system for the identified composition patterns. It also presents composition rules for deriving systemic trust values for each composition pattern. Lastly, results from applying the composition patterns to a case study show our trust composition model can predict trust of a composed system with 55%-70% uncertainty that increases with system complexity.

Figure 4. Application View of "Trustworthiness Modeling in SW" Within the "TRUST" Concept Area.

The summary by concept of the full results is shown in Figure 5, with the worldwide number of research papers for each subcategory. Table 2 reflects current constraints in the data set (h-index not collected on all data), so shows the relative ranking of the top 3 countries based on ~10% of h-index data.

Appendix A shows the full results sorted by geographic area of interest.

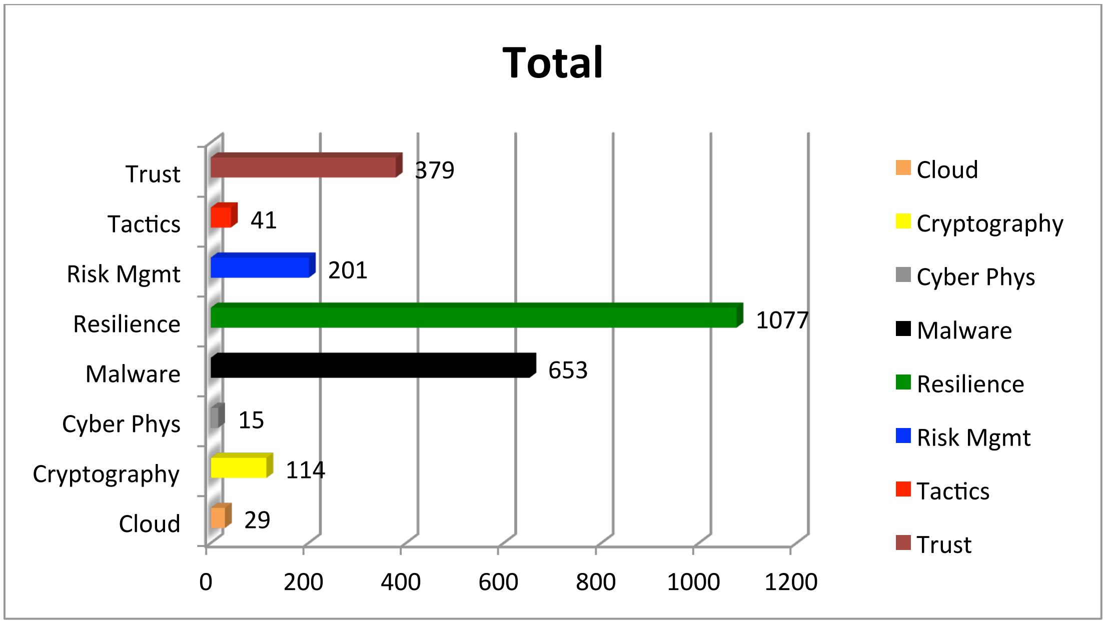


Figure 5. Results by Summary Concept Area

Distribution Code A: Approved for public release; distribution is unlimited.

Table 2. (Preliminary) Top 3 Quality Providers (normalized h-index)

Country	h(n)-index*
Germany	1.30
USA	1.29
South Korea	1.10
*Normalized, linear 1-5 scale	

Appendix B provides results filtered to include those countries that are within the AOARD geographic areas of responsibility. In order to provide the details required to support AOARD interaction with researchers in these areas, abstracts are also included in the appendix.

The summary by concept of these filtered results is shown in Figure 6, with the number of research papers for each subcategory within the AOARD area of responsibility.

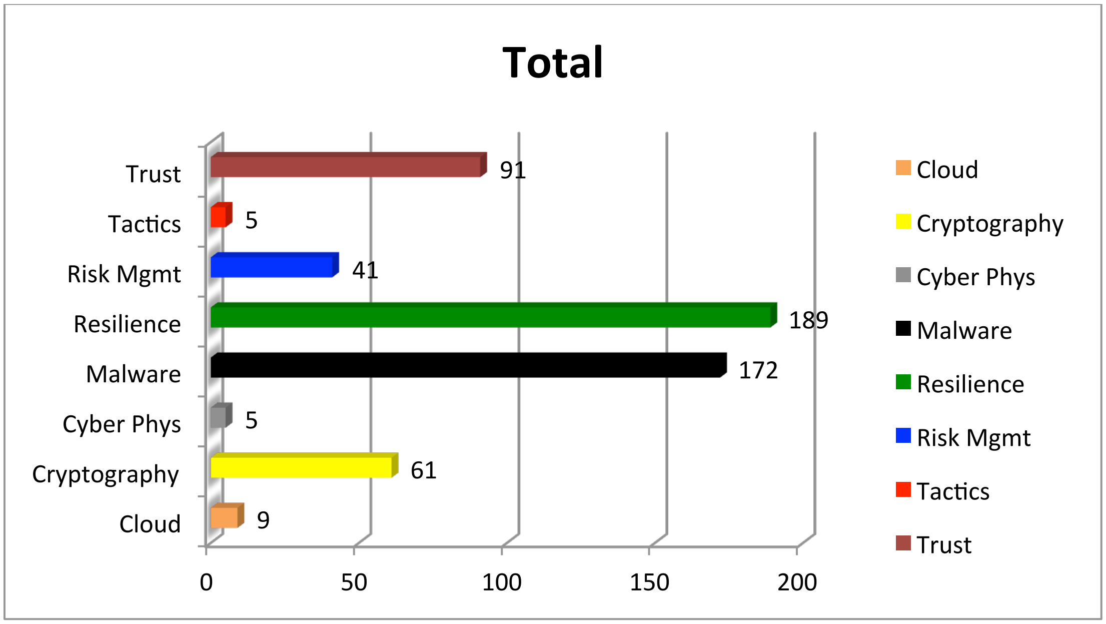


Figure 6. Results by Summary Concept Area Filtered by AOARD Area of Responsibility

Results Self-Assessment

Objective 1: Provide indications of relevant research areas, and match these areas to a thorough, engineering driven rationale for why AOARD would fund specific research pointed to by the results detailed in this proposal.
COMPLETE.

Objective 2: Provide related metrics that outline specific elements of the indicated research areas, identifying qualifications / past research of the subject researchers that identify them as emerging or pre-eminent leaders in Cyber research.

PARTIAL. Individual researcher data (primarily h-index) is available to the team, but at this point we have been unable to automate the extraction of the complete data set. We initially attempted to merge data using the “Publish or Perish” site to manually extract this h-index data. Since this was driven by Google Scholar, query limits made this time prohibitive. Subsequent data was added using additional (manual) pulls from Web of Science (Author searches, followed by selection of Citation Reports). This was more useful, though again, time constraints limited completeness of the data search effort. Also, for some (common/foreign) author names, it was difficult to determine based on name variations, if the h-index was being correctly computed on a single author. As a result, some of the h-indexes may be higher than actuals for the authors. Additional time is required in order to incorporate more complete and precise h-index data into the project.

Objective 3: Establish a collaborative web-based set of tools that will support AOARD personnel in enhancing collaborative communication of the key research being studied and funded, sharing of research papers and concepts, and establishment of a shared vision of the strategic goals of the collaborators.
COMPLETE. Web-based tool (prototype) delivered to AOARD personnel. On-line data is available at http://cims.enovations.org. Additional features would make this tool a more effective search tool to support AOARD staff in preparing for potential visits to universities, including review of abstracts and relative quality of research (based on the metrics developed in this study).

Objective 4: Deliver a demonstrated ontology that yields an operationally relevant and easily updateable set of descriptions and visualizations of shared insights and global trends in the cyber arena.
PARTIAL. This first iteration was delivered as visualizations of the ontology, and associated data graphs. However, results of OLLU staff refinements to the search functions used have not been incorporated into an automated search capability. This was deemed a capability that could be built as part of a follow-on or separate research effort. Follow-on efforts would likely include a hybridization of both ensemble learning techniques[5], and a more traditional concept-driven inferencing approach, based on natural language processing of technical abstracts.

Qualifications

Kevin Barton, Project Director (CISSP)
Mr. Barton is an Assistant Professor, Computer Information Systems and Security, at Our Lady of the Lake University. Mr. Barton holds a Master of Science in Information Systems and Security, and is a Ph.D. candidate in Information Systems with a concentration in Information Security. Mr. Barton has 32 years of experience in telecommunications, information technology, and information security. He has instructed graduate and undergraduate courses in information systems and information system security at a NSA/DHS designated CAE-IAE for 4 years. His research interests are information security management, information security governance, intrusion detection, and critical infrastructure cybersecurity.

Matthew A. Trippy, Co-Principal Investigator (PMP, CISSP, GPEN)
Mr. Trippy has previously led development efforts in Advanced Cyber Automated Testing using ontologies and concept mapping techniques similar to those described in this grant proposal. With over 24 years of experience in Systems Engineering, cyber research, and management and practice of both software and hardware projects, Mr. Trippy provides a deep and varied expertise to the subject problem set. He holds a Master of Science in Electrical Engineering, and Bachelor of Science in both Electrical Engineering and Applied Physics. During the last 15 years, he has been involved in various cyber efforts,

both in contract support roles to Department of Defense projects, as well as while serving active duty for the Joint Electronic Warfare Center.

Institution

Our Lady of the Lake University (OLLU), founded in 1895 by the Congregation of the Divine Providence, is a coeducational, Catholic, liberal arts, private institution with an enrollment of 2,764 (1517-undergraduates, 1247-graduate) as of the Fall 2012. A multi-site regional university, the main campus is located in San Antonio, Texas with additional off-site locations in Houston, and Harlingen, Texas. OLLU is accredited by the Southern Association of Colleges and Schools. OLLU is designated a postsecondary minority institution by the U.S. Department of Education ("United States Department of Education Accredited Postsecondary Minority Institutions," n.d.)

Computer Information Systems & Security (CISS) Department

The CISS department has five full time faculty members (three with doctoral degrees). Current faculty members are:

Carol Jeffries-Horner, PhD	Professor and Department Chair
Jesus Carmona, PhD	Assistant Professor
Murad Moqbel, PhD	Assistant Professor
Ted Ahlberg, MS	Assistant Professor
Kevin Barton, MS	Assistant Professor

OLLU offers three undergraduate degrees in CISS. The Bachelor of Business Administration and Bachelor of Science both have a security track. The security track is by far the most popular track for undergraduate degrees. Both degrees require 120 credit hours, including a shared core curriculum in CISS. Four security courses totaling 12 credit hours are required for the security track. A Bachelor of Applied Studies is also offered.

References

1) Adler, R., Ewing, J., and Taylor, P. (2008) Citation statistics. A report from the International Mathematical Union. www.mathunion.org/publications/report/citationstatistics0.

2) Schryen, G. (2010). A fuzzy model for IT security investments. *Proceedings of Sicherheit, Schutz und Zuverlässigkeit (SICHERHEIT 2010)*. Berlin.

3) United States Department of Education Accredited Postsecondary Minority Institutions. (n.d.).*U.S. Department of Education*. Retrieved January 8, 2013, from http://www2.ed.gov/about/offices/list/ocr/edlite-minorityinst-list-tab.html

4) Watters, P. A., Layton, R., & Dazeley, R. (2011). How much material on BitTorrent is infringing content? A case study. *Information Security Technical Report*, *16*(2), 79–87. doi:10.1016/j.istr.2011.10.001

5) Zhang, Cha & Ma, Yunqian, Editors. Ensemble Machine Learning: Methods and Applications, Springer 2012, New_York, Dordrecht, Heidelberg, London